

Efficient image encryption scheme with synchronous substitution and diffusion based on double S-boxes

Xuan-Ping Zhang(张选平), Rui Guo(郭瑞), Heng-Wei Chen(陈恒伟),Zhong-Meng Zhao(赵仲孟), Jia-Yin Wang(王嘉寅)

Citation: Chin. Phys. B . 2018, 27(8): 080701. **doi:** 10.1088/1674-1056/27/8/080701

Journal homepage: http://cpb.iphy.ac.cn; http://iopscience.iop.org/cpb

What follows is a list of articles you may be interested in

Visibility enhancement in two-dimensional lensless ghost imaging with true thermal light

Xi-Hao Chen(陈希浩), Ling Yan(燕玲), Wei Wu(吴炜), Shao-Ying Meng(孟少英), Ling-An Wu(吴令安), Zhi-Bin Sun(孙志斌), Chao Wang(王超), Guang-Jie Zhai(翟光杰)

Chin. Phys. B . 2017, 26(6): 060702. **doi:** 10.1088/1674-1056/26/6/060702

Anisotropic total variation minimization approach in in-line phase-contrast tomography and its application to correction of ring artifacts

Dong-Jiang Ji(冀东江), Gang-Rong Qu(渠刚荣), Chun-Hong Hu(胡春红), Bao-Dong Liu(刘宝东), Jian-Bo Jian(简建波), Xiao-Kun Guo(郭晓坤)

Chin. Phys. B . 2017, 26(6): 060701. **doi:** 10.1088/1674-1056/26/6/060701

Coupling of two-dimensional atomistic and continuum models for dynamic crack

Ren Guo-Wu, Tang Tie-Gang

Chin. Phys. B . 2014, 23(11): 118704. **doi:** 10.1088/1674-1056/23/11/118704

Third-order optical intensity correlation measurements of pseudo-thermal light

Chen Xi-Hao, Wu Wei, Meng Shao-Ying, Li Ming-Fei

Chin. Phys. B . 2014, 23(9): 090701. **doi:** 10.1088/1674-1056/23/9/090701

Efficient image encryption scheme with synchronous substitution and diffusion based on double S-boxes*

Xuan-Ping Zhang(张选平), Rui Guo(郭瑞), Heng-Wei Chen(陈恒伟), Zhong-Meng Zhao(赵仲孟), and Jia-Yin Wang(王嘉寅)†

School of Electronic and Information Engineering, Xi'an Jiaotong University, Xi'an 710049, *China*

(Received 11 February 2018; revised manuscript received 11 April 2018; published online 10 July 2018)

Single or multiple S-boxes are widely used in image encryption schemes, and in many image encryption schemes the asynchronous encryption structure is utilized, which separates the processes of substitution and diffusion. In this paper, we analyze the defects of this structure based on the example of an article and crack it using a simpler method. To address the defects of the asynchronous encryption structure, a novel encryption scheme is proposed, in which the structure of synchronous substitution and diffusion based on double S-boxes is utilized, so the processes of substitution and diffusion are combined together and the attackers cannot crack the cryptosystem by any of the processes. The simulation results and security analysis show that the proposed encryption scheme is safer and more efficient to expediently use in the real-time system.

Keywords: image encryption, S-box, crack, synchronous substitution and diffusion

PACS: 07.05.Pj, 87.57.N–, 87.57.C– **DOI:** 10.1088/1674-1056/27/8/080701

1. Introduction

During the past decade, the rapid growth of the internet has promoted a great deal of information to be generated, of which images occupy a large proportion. Research on the image is a very hot topic.[1–3] Therefore, the security issues of images have received more and more attention; however, traditional encryption algorithms are typically designed for textual information and have been found to be unsuitable for image encryption due to some intrinsic features of images such as high pixel correlation and redundancy.[4] Then, some image encryption schemes based on Chaos,[5–8] one-time keys,[9,10] bit-level,[11–13] DNA rule,[14–16] and frequency domain[17,18] are proposed. For example, in Ref. [5], a chaotic image encryption scheme based on a perceptron model was proposed, while the high-dimension Lorenz system and a neural network were used in the encryption scheme to improve the security of the cryptosystem. In Ref. [9], the authors proposed a color image encryption based on one-time keys and robust chaotic maps. They utilized the MD5 and combined the algorithm with the traditional cycle encryption to ensure higher security. In Ref. [11], the authors proposed a color image encryption by using a spatial bit-level permutation and high-dimensional chaotic system. The plain image was transformed into a binary matrix and encrypted based on the bit-level, so the encryption scheme achieved a good encryption result and the key space was large enough. In Ref. [14], the authors proposed an image encryption by using DNA complementary rule and chaotic maps. The plain image was encoded into four nucleotides by the deoxyribonucleic acid (DNA) coding, and the initial conditions of the chaotic maps were changed automatically in every encryption process. In the above encryption methods, chaos is widely applied to image encryption, since it is characterized in aperiodicity, pseudo-randomness, and high sensitivity to initial values and parameters.

Recently, many image encryption schemes were proposed based on chaos.[19–25] For example, in 2017, Wu *et al.*[19] proposed a color image encryption based on chaotic systems and an elliptic curve ElGamal scheme. The authors designed an asymmetric image encryption scheme for the advantages that the key groups and the number of keys in a secret information transmission among multiple people were very small, and the key transmission mode was relatively simple and secure. Chai *et al.*[20] proposed an image encryption scheme based on three-dimensional (3D) Brownian motion and chaotic system. It utilized the block confusion based on 3D Brownian motion and position sequence group (BCBPSG), which effectively improved the statistical performance of the algorithm. Ye *et al.*[21] proposed a self-cited pixel summation based image encryption algorithm. Because of the sensitivity of the chaotic map to its initial condition and the plain-image-dependent key stream, any tiny change in the secret key or the plain image would lead to a significantly different cipher image. In 2018, Parvaz and Zarebnia[22] proposed a novel color image encryption scheme. They defined a combined chaotic system which had good properties, and the combined chaotic system was effectively applied to the cryptosystem. Ullah *et al.*[23] proposed a novel scheme for image encryption by using a substitution box and chaotic system. The substitution box was constructed

*Project supported by the Natural Science Foundation of Shaanxi Province, China (Grant No. 2014JM8322).

†Corresponding author. E-mail: wangjiayin@mail.xjtu.edu.cn

© 2018 Chinese Physical Society and IOP Publishing Ltd

by a new method, and the encryption scheme exhibited outstanding diffusion as well as confusion properties.

The typical image encryption structure based on chaos is of permutation-substitution. The process of permutation changes the position of the pixels in the image. But the permutation-only encryption scheme is unsafe, because the pixels in the image are unchanged, and the attackers can obtain the equivalent permutation matrix by the chosen-plaintext attack. So the structure of permutation-substitution is widely used, while the process of substitution changes the pixel values to improve the security of cryptosystem.

Many image encryption schemes substitute the pixels by the single or multiple S-boxes, then diffuse the pixels to improve the effect of encryption.[26–29] However, some encryption schemes separate the processes of substitution and diffusion, namely, asynchronous substitution and diffusion scheme (ASAD). There are some potential defects based on the ASAD, for example, once the attackers obtain the equivalent key streams used in the diffusion, they can easily make the process of substitution useless and the whole encryption scheme is totally cracked. So the potential insecurity is caused by the separated processes of substitution and diffusion. Some encryption schemes based on the ASAD proved to be unsafe and suffered attack. For instance, in Ref. [26], an image encryption scheme based on a hyper-chaotic system and dynamic S-box was proposed, which permuted and substituted the plain image to obtain the substituted image firstly, and then diffused the substituted image to obtain the cipher image. However, the diffusion process revealed information about the substituted image, which resulted in the attackers easily recovering the substituted image.[30] In Ref. [27], a novel chaotic diffusion was added into the existing process of substitution, and the encrypted images with different gray scales were totally confused, but it was cracked in Ref. [31], which cracked the diffusion process to obtain the substituted image without the first block by the ciphertext-only attack, then totally restored the cipher image by the chosen-plaintext attack. In Ref. [32], the authors pointed out the defects of the diffusion process in an encryption scheme, which was based on a new mapping rule. So the structure of ASAD is actually unsafe.

In this paper, we analyze an encryption scheme described in Ref. [27] to explain the defects of ASAD, and crack the encryption scheme by using a simpler method than the method in Ref. [31]. Then a novel image encryption scheme is proposed to address the defects of ASAD. To improve the security of the encryption scheme further, the pixels in the plain image are encrypted twice by the double S-boxes, so the relationship between two encryption steps is enhanced, while the parameters used in the different S-boxes can influence each other. Also, the novel encryption scheme combines the processes of substitution and diffusion, so the encryption structure is synchronous, and the defects of the ASAD are addressed in the novel encryption scheme. Meanwhile, the efficiency of the novel encryption scheme is enormously high compared with other encryption schemes.

The rest of this paper is organized as follows. The example of ASAD in Ref. [27], the attack method in Ref. [31], and a simple attack method are described in Section 2. The novel encryption scheme based on synchronous substitution and diffusion is described in Section 3. The simulation results and security analysis are provided in Section 4. Finally, some conclusions are drawn from the present study in Section 5.

2. Example of ASAD and attack method

2.1. Example of ASAD

In this subsection, the example of ASAD in Ref. [27] is described. The sketch of the encryption scheme is shown in Fig. 1, and the encryption steps are described as follows.

Step 1 The chaotic map used in Ref. [27] is a logistic map, which is defined as

$$x_{n+1} = \mu x_n (1 - x_n), \tag{1}$$

where the initial parameter is $\mu \in [3.57, 4]$, the system is chaotic, and the $x_n \in (0, 1)$.

Step 2 The size of the plain image is $M \times N$. The MN pseudo random numbers $\{d_i\}$ $(i = 0, 1, 2, \ldots, MN-1)$ are obtained by Eq. (1) and the numbers ranging from 0 to 2 are obtained by the operations of discrete format and module, the $\{d_i\}$ denotes the distribution map.

Step 3 Construct three S-boxes, i.e., AES S-box, Gray S-box, and Hussain's S-box. The distribution map $\{d_i\}$ is used to map the pixels into one of the three S-boxes. Then the pixels in the plain image are substituted by the selected S-box, while the candidate elements in the S-boxes are decided by the pixels in the plain image. So the substituted image is obtained.

Step 4 Divide the substituted image into nonoverlapping blocks of $Z \times Z$ elements, then the size of $Z \times Z$ pseudo random numbers S are generated through the logistic map. The first block B'_1 in the cipher image is obtained by Eq. (2) where $\oplus$ is the bit-wise XOR operation and B_1 is the first block in the substituted image.

$$B'_1 = B_1 \oplus S. \tag{2}$$

Step 5 Each K-th $(K \geq 2)$ block in the substituted image is XORed with the $(K-1)$-th block in the cipher image. The process of encryption is described as follows:

$$\begin{cases} B'_2 = B'_1 \oplus B_2, \\ B'_3 = B'_2 \oplus B_3, \\ B'_K = B'_{(K-1)} \oplus B_k, \\ \quad \vdots \\ B'_L = B'_{(L-1)} \oplus B_L, \end{cases} \tag{3}$$

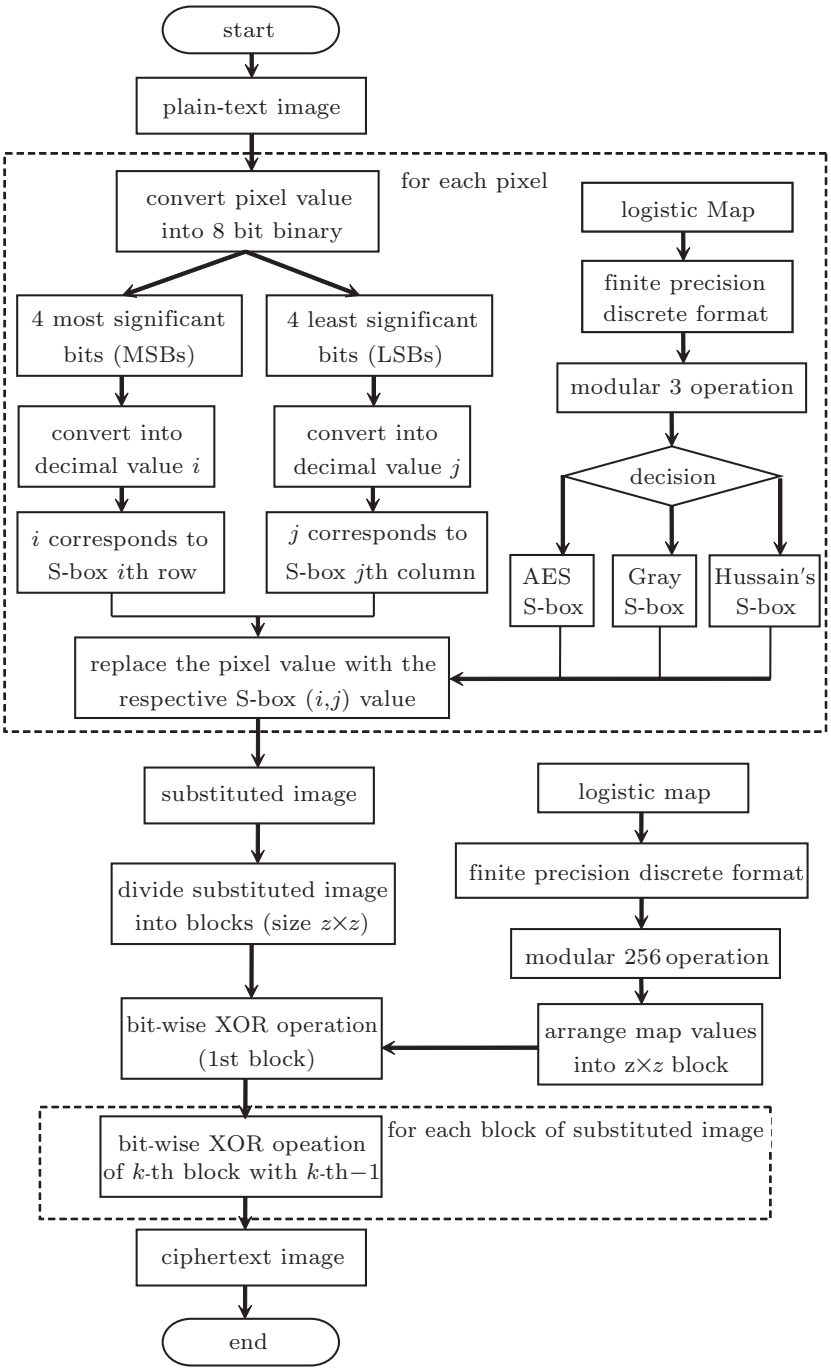


Fig. 1. Sketch of original scheme.

where B'_K represents the K-th obtained block in the cipher image, B_K the K-th block in the substituted image, and L the number of the blocks in the image. So the cipher image is obtained after the operation.

2.2. Potential defects of ASAD

The potential defects of the above encryption scheme based on ASAD are summed up as follows.

1) Unsafe diffusion process The diffusion process is easily cracked by the cipher-only attack, so the substituted image without the first block is obtained. The attack method is shown below.

$$\begin{cases} B_L = B'_{(L-1)} \oplus B'_L, \\ B_{(L-1)} = B'_{(L-2)} \oplus B'_{(L-1)}, \\ B_{(L-2)} = B'_{(L-3)} \oplus B'_{(L-2),} \\ \quad\vdots \\ B_K = B'_{(K-1)} \oplus B'_K, \\ B_2 = B'_1 \oplus B'_2. \end{cases} \tag{4}$$

2) Ineffective diffusion process While one pixel is changed in the plain image, there are few changed pixels in the cipher image. So the encryption scheme cannot resist the chosen-plaintext attack.

3) Separated processes of substitution and diffusion While the diffusion process is unsafe and unrelated to the substitution, the attackers can crack the diffusion process and obtain the equivalent key streams first, then the process of substitution is useless and the whole encryption scheme is cracked.

2.3. Simple attack

The encryption scheme in Ref. [27] was attacked in Ref. [31] and described as follows. Firstly, the substituted image without the first block was obtained by the cipher-only attack shown in Eq. (4). Then the distribution map $\{d_i\}$ ($i = Z$, $Z+1, \ldots, MN-1$) without the first block and mappings of the three S-boxes used in the substitution were obtained. So far, the substitution process was clear and the plain image without the first block was obtained. Finally, the distribution map $\{d_i\}$ ($i = 0, 1, \ldots, Z-1$) in the first block was obtained to restore the chaotic block S used in the diffusion, so the process of diffusion was clear and the plain image was recovered totally.

The novel attack method simplifies the process of cryptanalysis compared with the attack method in Ref. [31], while it does not need to know the whole distribution map $\{d_i\}$ and the three S-boxes used in the substitution process. As shown in Eq. (2), the first block in the cipher image is obtained by the bit-wise XOR operation. The two processes of substituting the pixels by S-boxes and the bit-wise XOR operation based on chaotic block S can be equivalent to one mapping operation, so neither the first block in the substituted image nor S needs to be known. The novel attack method establishes the whole coding table T to reveal the correspondence between the pixels in the cipher image and plain image intuitively, so the pixels in the cipher image can easily find their corresponding plain pixels based on the coding table T. The total steps are described as follows.

Step 1 Obtain the size of block Z. Construct two images with the same pixels without the first pixel, then encrypt the two images to obtain the corresponding cipher images. According to the original encryption scheme for the first block shown in Eq. (2) and Section 2, there will be some different pixels between two cipher images, and the distance between the first and the second different pixels in the first row is the size of block.

Step 2 The 256 different images with all the same pixel values that range from 0 to 255 are transformed into the vector and encrypted, while the vector size is $1 \times L$, and the size of plain image is $M \times N$, $L = M \times N$. By using the ciphertext-only attack based on Eq. (4), the corresponding substituted image without the first block is obtained. As mentioned above, the first block in the substituted image does not need to be known. Then obtain the vector of the middle image, while the first block is to the same as the first block in the cipher image. The 256 middle images are combined and denoted as C', while $C'_i(j)$ is satisfied for $i \in [0, 255]$, $j \in [0, L-1]$.

Step 3 Construct the coding table T whose size is $256 \times L$. Set $i = 0$ and repeatedly iterate Eq. (5) for $j = 0, 1, \ldots, L-1$. Then set $i = i+1$ and repeat the above operations until i reaches 255. So the whole coding table T is obtained after the cycle.

$$T(C'_i(j))(j) = i. \tag{5}$$

Step 4 Recover the plain image. Assume that a cipher image C needs to be recovered. Firstly, the size of block Z is obtained by Step1. Then the middle image C' is obtained by the ciphertext-only attack based on the block size Z. The vector of the plain image is P in a size of $1 \times L$, for $j = 0, 1, \ldots, L-1$, the P is obtained based on coding table T by the following equation:

$$P(j) = T(C'(j))(j). \tag{6}$$

Transform the vector P into the size $M \times N$, and the plain image will be obtained.

The computational complexity of the novel attack method of obtaining the coding table T is 257 times that of the encryption and cipher-only attack, so the time spent is acceptable.

The result of the crack experiment is shown in Fig. 2 based on the different images, like Lena, Peppers, and Baboon. There is no difference between the original images and recovered images, so the novel attack method is effective.

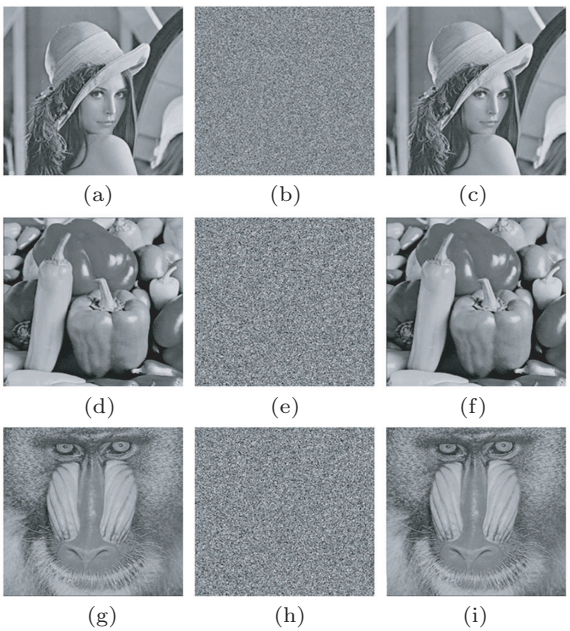


Fig. 2. (color online) (a) Original, (b) encrypted, and (c) recovered Lena; (d) original, (e) encrypted, and (f) recovered Peppers; (g) original, (h) encrypted, and (i) recovered Baboon.

3. Novel encryption scheme

In the original encryption scheme, the authors encrypted the pixels based on ASAD and the encryption scheme proved to be unsafe and cracked. The main defects of the ASAD

are that the processes of substitution and diffusion are separated, then the diffusion process is ineffective and unsafe. So the encryption scheme based on ASAD has potential security risks, while the attackers can crack the process of the diffusion first, and the substitution process has no relationship with the diffusion process, so the process of substitution is also easily cracked and the whole encryption scheme is unsafe.

To overcome the defects of ASAD, a novel encryption scheme is proposed. The main ideas of the encryption scheme are reflected in the three aspects as follows. (i) To improve the security of the encryption scheme, the pixels are encrypted twice by double S-boxes, and the parameters used in different encryption steps can influence each other and be dynamically updated, so the two processes of encryption are contacted closely. (ii) The two processes of substitution and diffusion are combined by double S-boxes, so the encryption structure is synchronous and not separated. As a result, the defects of the ASAD are addressed. (iii) The forward and backward encryption are used to improve the security of the cryptosystem further, and the initial encryption position is denoted as a secret key to enlarge the key space. Based on the above encryption ideas, the attackers cannot gradually crack the cryptosystem by any of the processes of substitution and diffusion, so the encryption scheme is safe enough.

According to the above encryption ideas, we design the encryption scheme, and the sketch of the novel encryption scheme is shown in Fig. 3, the main encryption algorithm is shown in Eqs. (7) and (8).

$$\begin{cases} t_i = S_1[P_i \oplus cxor], \\ c_i = S_2[(t_i + csum)\%256], \end{cases} \tag{7}$$

$$\begin{cases} cxor = c_i \oplus cxor, \\ csum = (t_i + csum)\%256, \end{cases} \tag{8}$$

where % is the remainder that returns after division; parameters of *cxor* and *csum* are denoted as the secret keys; *cxor* and *csum* $\in [0, 255]$; S_1 and S_2 are two different S-boxes; P_i is the pixel in the plain image; C_i is the pixel in the encrypted image.

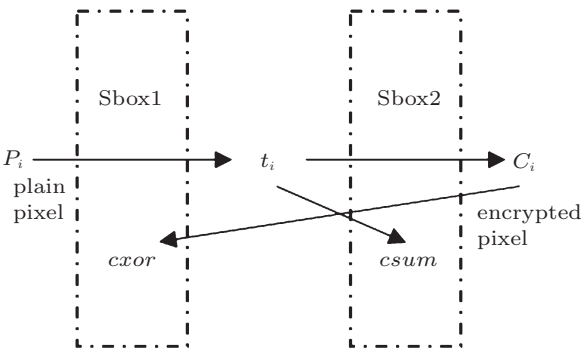


Fig. 3. Sketch of novel encryption scheme.

The total encryption steps are described as follows.

Step 1 Transform the plain image into a vector P in a size of $1 \times L$, while the size of plain image is $M \times N$ and $L = M \times N$, then perform the forward encryption.

Step 2 Construct two different S-boxes named S_1 and S_2. Set $i = pos$ and calculate Eq. (7), while *pos* is denoted as a secret key, and $pos \in [0, L-1]$. Update the parameters *cxor* and *csum* by Eq. (8).

Step 3 Set $i = i+1$, and repeatedly calculate Eqs. (7) and (8) until i reaches $L-1$. Then encrypt the remaining pixels in P. Set $i = 0$, repeat the above steps until i reaches *pos*-1. So the encryption process in the forward direction is finished.

Step 4 Perform the backward encryption. The initial parameters of *cxor* and *csum* are given the new values and denoted as the secret keys, and the double S-boxes are constructed again. Then repeat the above encryption processes to update the pixels based on the opposite iteration direction, while i changes from *pos*-1 to 0 first, and then changes from L-1 to *pos*.

Step 5 Transform the vector C into the size $M \times N$ and the cipher image is obtained.

In the decryption process, assume that the S_1^{-1} and S_2^{-1} are inversed S_1 and S_2, where $S^{-1}(S(P)) = P$. The decryption process is described as follows:

$$\begin{cases} t_i = \left(S_2^{-1}[c_i] - csum + 256\right)\%256, \\ p_i = S_1^{-1}[t_i] \oplus cxor. \end{cases} \tag{9}$$

After decrypting a pixel c_i, update the parameters *cxor* and *csum* by Eq. (8).

4. Experiment results and security analyses

In this section, the different images are used to evaluate the encryption effect of the proposed algorithm. All the simulations are performed on a personal computer with intel (R) Core(TM) i5-2400 CPU, 3.10 GHz, 8.00 G memory, and 450-GB hard disk with a Window 7 operating system, and the compile platform is the Visual Studio of version 2013.

For the comparison purpose, we employ three encryption schemes in Refs. [6], [13], and [16], while the encryption schemes in Refs. [6], [13], and [16] are based on the chaos, bit-level, and DNA rule respectively. Therefore, this comparison can exhibit the differences among the performances obtained by applying different encryption methods.

4.1. Experimental results

To show the security and efficiency of the proposed algorithm, we use eight gray images each with a size of 512×512 as the original ones, i.e., the 'Lena', 'Peppers', 'Baboon' , 'Boat', 'Bridge', 'Lake', 'White', and 'Black' images.

Figure 4 shows the original plain-images. The corresponding encrypted and decrypted images are displayed in

Figs. 5 and 6, respectively. As can be seen, the cipher-images are completely disordered and unrecognizable. The decrypted images are identical to the corresponding original ones. After the test, no difference is shown between the plain images and the decrypted images. Therefore, our proposed algorithm has a good encryption effect.

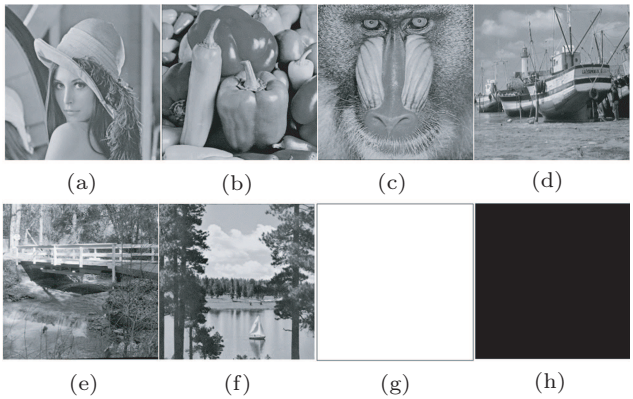


Fig. 4. Original images: (a) Lena plain-image; (b) Peppers plain-image; (c) Baboon plain-image; (d) Boat plain-image; (e) Bridge plain-image; (f) Lake plain-image; (g) White plain-image; (h) Black plain-image.

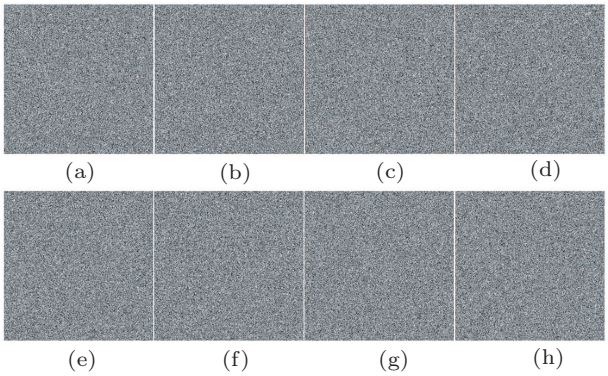


Fig. 5. Cipher-images: (a) Lena cipher-image; (b) Peppers cipher-image; (c) Baboon cipher-image; (d) Boat cipher-image; (e) Bridge cipher-image; (f) Lake cipher-image; (g) White cipher-image; (h) Black cipher-image.

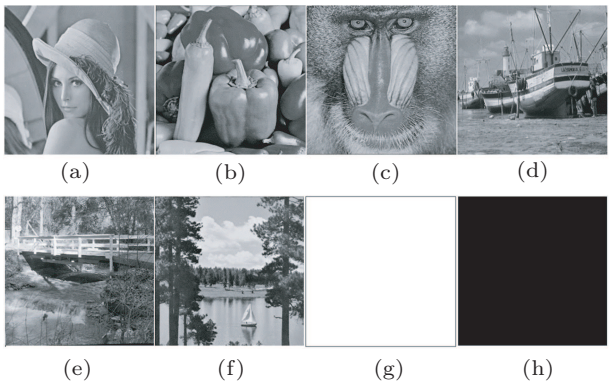


Fig. 6. The decrypted images: (a) Decrypted image of Lena; (b) Decrypted image of Peppers; (c) Decrypted image of Baboon; (d) Decrypted image of Bridge; (e) Decrypted image of Boat; (f) Decrypted image of Lake; (g) Decrypted image of White; (h) Decrypted image of Black.

4.2. Key space analysis

An effective image encryption scheme should have a large key space so that the brute-force attack is useless. In the proposed encryption scheme, the secret keys include two initial values x_1 and x_2 and parameter μ to generate the double S-boxes, two parameters *cxor*, *csum* used in forward encryption. Then the values used in backward encryption are different, named x_3, x_4, μ', *cxor*′, and *csum*′, so the minimum number of secret keys is eleven when the secret key *pos* is added. Suppose that the calculation precision of the computer is set to be 10^{-14}, so the total key space is at least 10^{96}, and it is large enough to resist all types of brute-force attack.

4.3. Histogram analysis

A good encryption scheme should make the histogram of an encrypted image as flat as possible. The histograms of the Lena and the cipher image are shown in Fig. 7, and it is clear that the histogram of the cipher image is uniformly distributed.

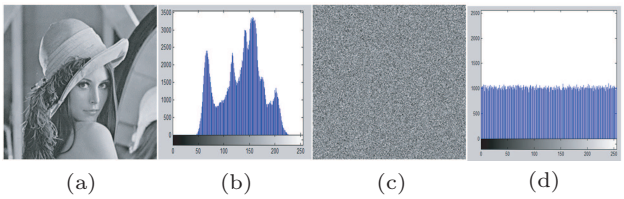


Fig. 7. (color online) Histograms of plain and encrypted Lena.

The variances of histograms are used to evaluate the uniformity of ciphered images. The lower value of variances indicates the higher uniformity of ciphered images. Then two variances of ciphered images, which are encrypted by different secret keys on the same plaintext image are also calculated, and the two values of variances being closer to each other indicates the higher uniformity of ciphered images when the secret keys are varying.[33] The variance of histogram is presented as follows:

$$\mathrm{Var}(Z) = \frac{1}{n^2}\sum_{i=1}^{n}\sum_{j=1}^{n}\frac{1}{2}(z_i - z_j)^2, \tag{10}$$

where Z is the vector of the histogram values and $Z = \{z_1, z_2, \ldots, z_{256}\}$, z_i and z_j being the numbers of pixels whose gray values are equal to i and j respectively.

In simulating experiments, two variances of histograms of two ciphered images by Eq. (10) from the same plain image with different secret keys are calculated. Only one parameter of secret keys is changed in such different secret keys.

The eight plain images shown in Fig. 4 are tested. In Table 1 the variances of histograms of ciphered images are listed. The parameters of x_3, x_4, μ', *cxor*′, and *csum*′ used in the backward encryption are mirrored with the parameters used in the forward encryption, so the parameters of x_1, x_2, μ, *cxor*, and *csum* are tested. In Table 1, the variances in the first column are obtained by the secret key x_1, the variances in the next column are obtained by only changing one parameter of x_2, μ, *cxor*, and *csum* respectively compared with the secret key x_1.

Table 1. Comparison among variances of histograms of all secret keys in the proposed algorithm.

Cipher image	x_1	x_2	μ	*cxor*	*csum*
Lena	1128.0469	816.6719	943.8203	959.3984	943.7422
Peppers	1079.4219	1019.3578	1097.8828	932.8203	999.5781
Baboon	954.2891	980.3705	1045.2578	1055.5938	874.5078
Boat	1148.5469	1005.4844	1000.1094	1072.0312	952.5547
Bridge	1067.4971	980.5649	1149.4971	1031.9717	931.1649
Lake	1064.4971	1164.8594	1094.4688	962.1797	910.2597
White	1087.7031	1048.1953	1153.4375	1149.9531	996.7188
Black	1020.2813	1061.1953	876.4844	990.1016	913.0469
Average	1068.7340	1009.5874	1045.1198	1019.2562	940.1966

The variance values are about 5000, which indicates that the average fluctuation of the number of pixels in each gray value is about 70 pixels. However, the variance value is 625571.4908 for the histogram of the plain image Lena. It is obvious that the proposed algorithm is effective.

To measure the uniformity of each parameter in secret keys, we calculate the percentage of variance differences between the x_1 and the secret key that only one parameter is changed compared with x_1. Each parameter such as x_2, μ, *cxor*, and *csum* for three plain images is calculated and listed in Table 2. As Table 2 shows, the key *cxor* leads to the closest uniformity, and the key x_2 leads to more fluctuation than other keys.

Table 2. Comparison among percentages of variances difference of histograms of secret keys in the proposed algorithm.

Cipher image	x_1/%	x_2/%	μ/%	*cxor*/%	*csum*/%
Lena	13.32	17.97	5.19	3.63	5.20
Peppers	7.54	1.56	9.38	7.06	0.41
Baboon	3.49	0.64	5.93	6.98	11.37
Boat	1.23	12.82	13.43	5.82	19.09
Bridge	6.74	1.94	14.95	3.20	6.88
Lake	8.52	18.79	11.62	1.88	7.17
White	14.53	18.72	4.32	13.42	4.26
Black	16.69	19.90	3.02	14.15	5.90
Average	9.01	11.54	8.48	7.01	7.54

To measure the histogram difference against plain images, the variance values among three images are changed obviously in Table 2. The difference in variance value indicates that the histogram depends on the plain image in the proposed algorithm. The simulation results indicate that any statistical attacks on the proposed scheme are useless.

4.4. Correlation analysis

The natural image has a high correlation with adjacent pixels, so the encryption scheme should effectively reduce the correlation in the encrypted image. In order to analyze the correlation with the adjacent pixels in the plain and cipher images, 2000 pairs of adjacent pixels are randomly chosen in the horizontal, vertical, and diagonal direction from the plain images and cipher images. The correlation distribution is shown in Fig. 8 and it is clear that the correlation among the adjacent pixels can be reduced greatly by the proposed encryption scheme.

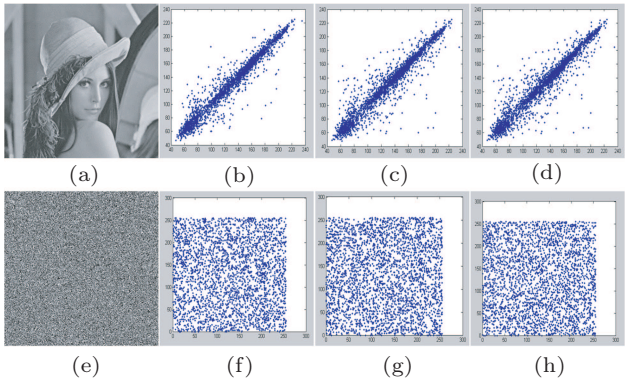


Fig. 8. (color online) Correlation analysis: (a) plain image and its (b) horizontal, (c) vertical, and (d) diagonal correlation; (e) encrypted image and its (f) horizontal, (g) vertical, and (h) diagonal correlation.

In order to calculate the correlation coefficient γ_{xy} of the adjacent pixels, we use the following formulas:

$$\begin{cases} \gamma_{xy} = \dfrac{cov(x,y)}{\sqrt{D(x)D(y)}}, \\ cov(x,y) = \dfrac{1}{N}\sum\limits_{i=1}^{N}(x_i - \bar{x})(y_i - \bar{y}), \\ D(x) = \frac{1}{N}\sum\limits_{i-1}^{N}(x_i - \bar{x})^2, \end{cases} \tag{11}$$

where x_i and y_i are the two adjacent pixels, and N is the total number of the adjacent pixel pairs selected from the image. The γ_{xy} of plain images, the proposed algorithm, and the algorithms in Refs. [6], [13], and [16] are shown in Table 3. It is obvious that the correlation coefficients of the plain images are very high while the encrypted images are close to zero. Then the absolute values of all correlation coefficients in the proposed algorithm are close to those from the algorithms in Refs. [6], [13], and [16].

Table 3. Correlations between the plain images and the encrypted images.

Algorithm	Horizontal	Vertical	Diagonal
Plain image (Lena)	0.9719	0.9850	0.9639
Proposed algorithm	0.0014	0.0011	0.0023
Ref. [6]	0.0019	0.0038	−0.0019
Ref. [13]	0.0024	−0.0006	0.0012
Ref. [16]	0.0020	−0.0007	−0.0014

4.5. Information entropy analysis

The information entropy is defined to express the degree of uncertainty or randomness in a given system. The information entropy $H(m)$ of an image is calculated from

$$H(m) = \sum_{i=0}^{N} p(m_i)\log_2\frac{1}{p(m_i)}, \tag{12}$$

where N is the total number of symbols, $m_i \in m$, and $p(m_i)$ represents the probability of the symbol m_i. For a random

image with 256 gray levels, the entropy ideally should be 8, so an effective encryption scheme should produce an encrypted image with the entropy close to 8. We use Eq. (12) to calculate the information entropies of the plain images and the encrypted images, and results are compared with those in Refs. [6], [13], and [16]. The results are shown in Table 4. It is clear that the entropies of encrypted images are very close to the theoretical optimal values, so that the proposed encryption scheme can produce encrypted images with good randomness.

Table 4. Comparison of entropy between plain images and encrypted images.

Image	Plain image	Cipher image	Ref. [6]	Ref. [13]	Ref. [16]
Lena	7.4455	7.9992	7.9971	7.9972	7.9970
Peppers	7.5715	7.9993	7.9972	7.9971	7.9970
Baboon	7.3585	7.9992	7.9974	7.9973	7.9969
Boat	7.1914	7.9992	7.9971	7.9970	7.9971
Bridge	5.7056	7.9994	7.9970	7.9971	7.9971
Lake	7.4845	7.9995	7.9970	7.9972	7.9970
White	0	7.9997	7.9970	7.9972	7.9971
Black	0	7.9998	7.9972	7.9971	7.9970

4.6. Differential attack analysis

To resist the differential attack, an effective encryption scheme should be sensitive to the change of plain image. The number-of-pixels changing rate (NPCR) and the unified average changing intensity (UACI) are used to evaluate the difference between two images. The NPCR and UACI are calculated by Eqs. (13), (14), and (15).

$$NPCR = \frac{\sum_{i,j} D(i,j)}{H \times W} \times 100\%, \tag{13}$$

$$D(i,j) = \begin{cases} 1, & \text{if } c_1(i,j) \neq c_2(i,j), \\ 0 & \text{if } c_1(i,j) = c_2(i,j), \end{cases} \tag{14}$$

$$UACI = \frac{1}{H \times W} \sum_{i,j} \frac{|c_1(i,j) - c_2(i,j)|}{255}, \tag{15}$$

where H and W represent the height and width of the cipher image, respectively; $C_1(i,j)$ and $C_2(ij)$ are the pixels in images C_1 and C_2, respectively. For two random images, the average *NPCR* is about 99.61%, and the average *UACI* is about 33.46%. We randomly change one pixel in the original plain image to obtain a modified image, and encrypt the original image and the modified image by the proposed encryption scheme with the same secret keys, then calculate the *NPCR* and *UACI* of the encrypted images. In this experiment, this test is performed 1000 times for each plain image, and the average, maximum, and minimum values of *NPCR* and *UACI* are given in Table 5. Then the comparison between *NRCR* and *UACI* based on the "Lena" image are shown in Table 6, which are compared with the results in Refs. [6], [13], and [16]. The values of *NRCR* and *UACI* proposed in Refs. [6] and [13] are calculated when encrypting images in two rounds.

From Tables 5 and 6, it is clear that the *NPCR* and *UACI* of the cipher images are close to the average *NPCR* and *UACI* of random images, respectively, so the proposed encryption scheme can resist the differential attack effectively. Then the performance of the proposed algorithm is better than those from the algorithms in Refs. [6] and [13], while the maximum value of *NRCR* is close to that from the algorithm proposed in Ref. [16].

Table 5. *NPCR* and *UACI* for different images based on the proposed algorithm.

Image	Average		Maximum		Minimum	
	NPCR/%	*UACI*/%	*NPCR*/%	*UACI*/%	*NPCR*/%	*UACI*/%
Lena	99.6106	33.4823	99.6498	33.6182	99.5783	33.3452
Peppers	99.6102	33.4534	99.6483	33.5835	99.5637	33.3464
Baboon	99.6104	33.4458	99.6547	33.5762	99.5862	33.3373
Boat	99.6105	33.4696	99.6478	33.5897	99.5758	33.3458
Bridge	99.6016	33.4539	99.6519	33.5679	99.5628	33.3578
Lake	99.6082	33.4587	99.6547	33.5764	99.5823	33.3497
White	99.6084	33.4814	99.6439	33.5846	99.5858	33.3735
Black	99.6109	33.4613	99.6352	33.5673	99.5957	33.3837

Table 6. Comparison between *NPCR* and *UACI*.

Algorithm	*NPCR*/%	*UACI*/%
Proposed algorithm	99.61	33.48
Ref. [6]	99.59	33.25
Ref. [13]	99.58	27.35
Ref. [16]	99.65	33.48

4.7. Key sensitivity analysis

In the encryption scheme, the cipher image should totally change when there is a slight change in the secret keys. To test the key sensitivity of the proposed encryption scheme, we randomly choose two groups of secret keys with only one-bit difference to encrypt the plain image, respectively. Then, the *NPCR* and the *UACI* of the encrypted image are calculated. This test is performed 1000 times for each plain image, and the average, maximum, and minimum values of *NPCR* and *UACI* are shown in Table 7. The results show that the proposed encryption scheme is highly sensitive to any small change (i.e., onebit) in the secret keys.

Table 7. Key sensitivities of the proposed scheme.

Image	Average		Maximum		Minimum	
	NPCR/%	*UACI*/%	*NPCR*/%	*UACI*/%	*NPCR*/%	*UACI*/%
Lena	99.6125	33.4682	99.6458	33.6035	99.5825	33.3836
Peppers	99.6069	33.4725	99.6482	33.5826	99.5826	33.3415
Baboon	99.6125	33.4528	99.6362	33.5672	99.5725	33.3273
Boat	99.6126	33.4628	99.6437	33.5725	99.5791	33.3415
Bridge	99.6056	33.4768	99.6418	33.5819	99.5849	33.3567
Lake	99.6058	33.4867	99.6458	33.5845	99.5871	33.3545
White	99.6036	33.4893	99.6417	33.5762	99.5726	33.3827
Black	99.6028	33.4527	99.6315	33.5636	99.5857	33.3747

4.8. Speed analysis

The encryption speed is an important factor for the encryption scheme to be widely used in the practical application. The proposed encryption scheme cannot be implemented in parallel forms, while the algorithms in Refs. [13] and [16] can be implemented in parallel to potentially enhance the computational efficiency. So the algorithms in Refs. [13] and [16] are replaced by other algorithms in the speed test. We run our encryption scheme 1000 times on 256 gray-scale images with the Lena image in a size of 256×256 and compare the average encryption efficiency with those of the algorithms proposed in Refs. [6] and [27] and Refs. [34]–[36]. The test results are listed in Table 8. It is clear that the proposed encryption scheme has higher efficiency.

Table 8. Comparison between encryption speeds cited from the literature and calculated by our proposed algorithm.

Algorithm	Ours	Ref. [34]	Ref. [35]	Ref. [6]	Ref. [36]	Ref. [27]
Speed/(m/s)	0.6634	1.5473	14.7249	2.3428	84.5806	1827.4854

4.9. Classical types of attacks

According to Kerchoff's principle,[37] the cryptosystem should be open and its security entirely depends on the secret key. In other words, the cryptanalyst can know everything about the cryptosystem without the secret key. A secure cryptosystem should resist all kinds of attacks; otherwise, the cryptosystem is insecure. Generally speaking, there are four classical types of attacks to break a cryptosystem, and their orders from the hardest types to the easiest types are listed as follows.

(I) Ciphertext attack: The opponent only possesses a series of ciphertexts.

(II) Known plaintext attack: The opponent only can possess a series of plaintext and corresponding ciphertexts.

(III) Chosen plaintext attack: The opponent can obtain the encryption machinery. Some plaintexts are chosen to encrypt and their corresponding ciphertexts can be obtained.

(IV) Chosen ciphertext attack: The opponent can obtain the decryption machinery. Some known ciphertexts are chosen to decrypt and their corresponding plaintexts can be obtained.

Obviously, the chosen plaintext attack is the most powerful attack. If a cryptosystem can resist this attack, it can resist other types of attacks.[38] The proposed encryption scheme combines the processes of substitution and diffusion by double S-boxes and the pixels encrypted by double S-boxes in different steps can influence each other. Meanwhile, the forward encryption and backward encryption are used to improve the security of a cryptosystem, so the attackers cannot gradually crack the encryption scheme by one of the S-boxes or the processes of substitution and diffusion. So the proposed encryption scheme can resist the chosen plaintext or ciphertext attack.

5. Conclusions

In this paper, an image encryption scheme based on asynchronous substitution and diffusion (ASAD) is described and some defects are pointed out, which makes the cryptosystem unsafe and cracked. Then a novel encryption scheme is proposed to address the defects in the ASAD. The pixels are encrypted twice by the double S-boxes, and the processes of substitution and diffusion are combined and synchronous. To improve the security of the cryptosystem further, the forward and backward encryption are also used in the encryption scheme. The simulation results and security analysis show that the proposed encryption scheme is safer and more efficient to expediently use in the real-time system.

References

[1] Chen B, Geng Z X, SHEN J and Yang Y 2009 *Chin. Phys. Lett.* **26** 040701
[2] Lu X W, Li J Z and Chen H Y 2010 *Chin. Phys. Lett.* **27** 104209
[3] Feng T, Yuan J, Yu Y, Zhou Y and Xu G 2013 *Chin. Phys. Lett.* **30** 100702
[4] Li X, Li C and Lee I 2016 *Signal Process* **125** 48
[5] Wang X Y, Yang L, Liu R and Kadir A 2010 *Nonlinear Dyn.* **62** 615
[6] Wang X Y, Liu L T, and Zhang Y Q 2015 *Opt. Laser. Eng.* **66** 10
[7] Sun J L, Liao X F, Chen X and Guo S W 2017 *Int. J. Bifurc. Chaos* **27** 1750073
[8] Li B, Liao X F and Jiang Y 2018 *Multimed. Tools Appl.* **77** 8911
[9] Liu H J and Wang X Y 2010 *Comput. Math. Appl.* **59** 3320
[10] Wang X Y and Teng L 2012 *Chin. Phys. B* **21** 020504
[11] Liu H J and Wang X Y 2011 *Opt. Commun.* **284** 3895
[12] Liu J Y, Yang D D, Zhou H B and Chen S H 2018 *Multimed. Tools Appl.* **77** 10217
[13] Zhang Y Q and Wang X Y 2015 *Appl. Soft Comput.* **26** 10
[14] Liu H J, Wang X Y and Kadir A 2012 *Appl. Soft Comput.* **12** 1457
[15] Pujari S, Bhattacharjee G and Bhoi S 2018 *Pro. Comp. Sci.* **125** 165
[16] Wang X Y, Zhang Y Q and Bao X M 2015 *Opt. Laser Eng.* **73** 53
[17] Zhang D, Liao X F, Yang B and Zhang Y S 2018 *Multimed. Tools Appl.* **77** 2191
[18] Yang B and Liao X F 2018 *Multimed. Tools Appl.* **77** 2191
[19] Wu J H, Liao X F and Yang B 2017 *Signal Process.* **141** 109
[20] Chai X L, Gan Z H, Yuan K, Lu Y and Chen Y R 2017 *Chin. Phys. B* **26** 020504
[21] Ye G D, Huang X L, Zhang Y and Zheng X Y 2017 *Chin. Phys. B* **26** 010501
[22] Parvaz R and Zarebnia M 2018 *Opt. Laser Eng.* **101** 30
[23] Ullah A, Jamal S S and Shah T 2018 *Nonlinear Dyn.* **91** 359
[24] Han F, Liao X F, Yang B and Zhang Y S 2018 *Multimed Tools Appl.* **77** 14285
[25] Rehman U A, Liao X F, Kulsoom A and Ullah S 2016 *Multimed. Tools Appl.* **75** 11241
[26] Liu Y, Tong X and Ma J 2016 *Multimed. Tools Appl.* **75** 7739
[27] Ahmad J and Hwang S O 2015 *Nonlinear Dyn.* **82** 1839
[28] Farwa S, Muhammad N, Shah T and Ahmad S 2017 *3d Research* **8** 26
[29] Tian Y and Lu Z 2017 *AIP Advances* **7** 085008
[30] Zhang X P, Nie W G, Ma Y L and Tian Q Q 2017 *Multimed. Tools Appl.* **76** 1
[31] Li M, Liu S, Niu L and Liu H 2016 *Opt. Laser Tech.* **86** 33
[32] Wu J H, Liao X F and Yang B 2018 *Signal Process.* **142** 292
[33] Zhang Y Q and Wang X Y 2014 *Information Science* **273** 329
[34] Wang X and Wang Q 2014 *Nonlinear Dyn.* **75** 567
[35] Hu G, Xiao D, Zhang Y and Xiang T 2017 *Nonlinear Dyn.* **87** 1359
[36] Liu W, Sun K and Zhu C 2016 *Opt. Laser. Eng.* **84** 26
[37] Pareek N, Patidar V and Sud K 2005 *Commun. Nonlinear Sci. Num. Simul.* **10** 715
[38] Wang X Y, Teng L and Qin X 2012 *Signal Process.* **92** 1101